UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/680,599	10/06/2000	Richard R. Wessman	OR00-03802	1833

22835 7590 05/20/2004		EXAMINER
PARK, VAUGHAN & FLEMING LLP		BETIT, JACOB F
508 SECOND STREET		

ART UNIT	PAPER NUMBER
2175	16

PARK, VAUGHAN & FLEMING LLP
508 SECOND STREET
SUITE 201
DAVIS, CA 95616

DATE MAILED: 05/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

	Application No.	Applicant(s)
	09/680,599	WESSMAN, RICHARD R.
	Examiner	Art Unit
	Jacob F. Betit	2175

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 April 2004_.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _25-51_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _25-51_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

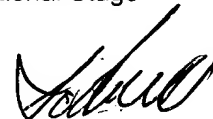8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**SAM RIMELL
PRIMARY EXAMINER**

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37

CFR 1.114. Applicant's Request for Continued Examination (RCE) submission filed on 16 April

2004 has been entered. In addition, the "After Final" amendment filed on 22 March 2004 has

been entered as a preliminary amendment for the continued examination of this application.

Remarks

2.   In response to communications filed on 22 March 2004, claims 25, 30, 34, 39, 43, and 48

are amended per applicant's request. Claims 25-51 are presently pending in the application.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 25, 34, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zizzi (U.S. patent No. 6,185,681) in view of McBride (U.S. patent No. 6,292,899 B1).

As to claim 25 Zizzi teaches a method for managing encryption within a database system,

wherein encryption is performed automatically and transparently to a user of the database system

(see abstract), the method comprising:

receiving a request at the database system to store data in the database system (see figure

4, step 415);

wherein the request is directed to storing data in a portion of the database system that has

been designated as encrypted (see figure 4 step 430, where the decision is "Yes");

in response to receiving the request:

automatically encrypting data within the database system using an

encryption function to produce an encrypted data (see figure 4, step 460); and

storing the encrypted data in the database system (see column 7, lines 15-21).

Zizzi does not teach creating a digest of data, wherein the digest is used to detect

tampering with the encrypted data, and wherein using the encryption function involves using an

encryption key recovered from an obfuscated copy of the keyfile within volatile memory.

McBride teaches a data security system that uses a volatile key apparatus to manage

access to a file (see abstract), in which he teaches creating a digest of data, wherein the digest is

used to detect tampering with the encrypted data (see column 6, lines 11-24, where "digest" is

read on "checksum"), and wherein using the encryption function involves using an encryption

key recovered from an obfuscated copy of the keyfile within volatile memory (see column 6,

lines 41-45).

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Zizzi to include creating a digest of data, wherein

the digest is used to detect tampering with the encrypted data, and wherein using the encryption

function involves using an encryption key recovered from an obfuscated copy of the keyfile

within volatile memory.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Zizzi by the teachings of McBride because creating a

digest of data, wherein the digest is used to detect tampering with the encrypted data would deter

tampering with the file (see McBride, column 6, lines 11-24), and because wherein using the

encryption function involves using an encryption key recovered from an obfuscated copy of the

keyfile within volatile memory would prevent access to the information that is encrypted (see

McBride, abstract).

As to claim 34, Zizzi teaches a computer-readable storage medium storing instructions

that when executed by a computer causes the computer to perform a method for managing

encryption within a database system, wherein encryption is performed automatically and

transparently to a user of the database system (see abstract, where "instructions" are read on

"software module", and it is inherent that the software must be stored on some medium), the

method comprising:

receiving a request at the database system to store data in the database system (see figure

4, step 415);

wherein the request is directed to storing data in a portion of the database system that has

been designated as encrypted (see figure 4, step 430, where the decision is "Yes");

in response to receiving the request:

automatically encrypting data within the database system using an

encryption function to produce an encrypted data (see figure 4, step 460); and

storing the encrypted data in the database system (see column 7, lines 15-21).

Zizzi does not teach creating a digest of data, wherein the digest is used to detect

tampering with the encrypted data, and wherein using the encryption function involves using an

encryption key recovered from an obfuscated copy of the keyfile within volatile memory.

McBride teaches creating a digest of data, wherein the digest is used to detect tampering

with the encrypted data (see column 6, lines 11-24, where "digest" is read on "checksum"), and

wherein using the encryption function involves using an encryption key recovered from an

obfuscated copy of the keyfile within volatile memory (see column 6, lines 41-45).

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Zizzi to include creating a digest of data, wherein

the digest is used to detect tampering with the encrypted data, and wherein using the encryption

function involves using an encryption key recovered from an obfuscated copy of the keyfile

within volatile memory.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Zizzi by the teachings of McBride because creating a

digest of data, wherein the digest is used to detect tampering with the encrypted data would deter

tampering with the file (see McBride, column 6, lines 11-24), and because wherein using the

encryption function involves using an encryption key recovered from an obfuscated copy of the

keyfile within volatile memory would prevent access to the information that is encrypted (see

McBride, abstract).

As to claim 43, Zizzi teaches an apparatus that facilitates managing encryption within a

database system, wherein encryption is performed automatically and transparently to a user of

the database system (see abstract), comprising:

a receiving mechanism that is configured to receive a request at the database system to

store data in the database system (see column 8, lines 32-41);

wherein the request is directed to storing data in a portion of the database system that has

been designated as encrypted (see figure 4, step 430, where the decision is "Yes");

an encrypting mechanism that is configured to automatically encrypt data within the

database system using an encryption function to produce an encrypted data (see column 9, lines

20-31) and;

a storing mechanism that is configured to store the encrypted data in the database system

(see column 7, lines 15-21).

Zizzi does not teach a digest creating mechanism configured to create a digest of the data,

wherein the digest is used to detect tampering with the encrypted data, and wherein using the

encryption function involves using an encryption key recovered from an obfuscated copy of a

keyfile within volatile memory.

McBride teaches a digest creating mechanism configured to create a digest of the data,

wherein the digest is used to detect tampering with the encrypted data (see column 6, lines 11-24,

where "digest" is read on "checksum"), and wherein using the encryption function involves using an encryption key recovered from an obfuscated copy of a keyfile within volatile memory (see column 6, lines 41-45).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi to include a digest creating mechanism configured to create a digest of the data, wherein the digest is used to detect tampering with the encrypted data, and wherein using the encryption function involves using an encryption key recovered from an obfuscated copy of a keyfile within volatile memory.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi by the teachings of McBride because a digest creating mechanism configured to create a digest of the data, wherein the digest is used to detect tampering with the encrypted data would deter the tampering with the file (see McBride, column 6, lines 11-24), and because wherein using the encryption function involves using an encryption key recovered from an obfuscated copy of a keyfile within volatile memory would prevent access to the information that is encrypted (see McBride, abstract).

5.   Claims 26-28, 30-33, 35-37, 39-42, 44-46, and 48-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zizzi (U.S. patent No. 6,185,681) in view of McBride (U.S. patent No. 6,292,899 B1) as applied to claims 25, 34, and 43 above, and further in view of Sutter (U.S. patent No. 5,924,094).

As to claims 26, 35, and 44, Zizzi as modified, teaches

wherein the encryption function uses a key stored in a keyfile managed by a security

administrator (see Zizzi, column 9, lines 25-30); and

wherein the encrypted data is stored using a storage function of the database system (see

Zizzi, column 9, lines 32-37).

Zizzi as modified, still does not teach wherein the portion of the database system that has

been designated as encrypted includes a column of the database system.

Sutter teaches wherein the portion of the database system that has been designated as

encrypted includes a column of the database system (see column 59, lines 10-16).

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Zizzi as modified, to include wherein the portion

of the database system that has been designated as encrypted includes a column of the database

system.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Zizzi as modified, by the teachings of Sutter because

wherein the portion of the database system that has been designated as encrypted includes a

column of the database system would keep unauthorized users from deciphering the encrypted

column of the database system.

As to claims 27, 36, and 45, Zizzi as modified, teaches further comprising:

receiving a request to retrieve data from the column of the database system (see Zizzi,

column 9, lines 44-59);

if the request to retrieve data is received from a database administrator, preventing the

database administrator from decrypting the encrypted data; if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting the encrypted data; and if the request to retrieve data is from an authorized user of the database system, allowing the authorized user to decrypt the encrypted data (see Zizzi, column 9, lines 40-43, where any user that does not have authorization to decrypt the data will not be authorized to decrypt it).

As to claims 28, 37, and 46, Zizzi as modified teaches data encryption standard (DES) and triple DES as a mode of encryption (see Zizzi, column 3, lines 29-37).

Zizzi as modified, still does not teach wherein the security administrator selects a mode of encryption for the column.

Sutter teaches wherein the security administrator selects a mode of encryption for the column (see column 59, lines 11-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi as modified, to include wherein the security administrator selects a mode of encryption for the column.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi as modified, by the teachings of Sutter because wherein the security administrator selects a mode of encryption for the column would allow the security manager to select various methods of encryption strengths depending on the importance of the file.

As to claims 30, 39, and 48, Zizzi as modified, teaches wherein managing the keyfile includes, but is not limited to:

establishing a relationship between a key identifier and he key stored in the keyfile (see Zizzi, column 6, lines 3-6);

storing the keyfile in one of,

an encrypted file in the database system, and a location separate from the database system (see Zizzi, column 6, lines 1-2);

Zizzi as modified, still does not teach creating the keyfile; establishing a plurality of keys to be stored in the keyfile; and moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

McBride teaches creating the keyfile; establishing a plurality of keys to be stored in the keyfile (see column 1, lines 6-10); and moving the obfuscated copy of the keyfile to the volatile memory within a server associated with the database system (see column 6, line 46-62).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi as modified, to include creating the keyfile; establishing a plurality of keys to be stored in the keyfile; and moving an obfuscated copy of the keyfile to a volatile memory within a server associated with the database system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zizzi as modified, by the teachings of McBride because creating the keyfile, and establishing a plurality of keys to be stored in the keyfile would safeguard the confidential data that is in the memory (see McBride, abstract); and because moving an obfuscated copy of the keyfile to a volatile memory within a server associated with

the database system would allow the user to access the encrypted data after the device has been

tampered with and the memory has been erased (see McBride, abstract).

As to claims 31, 40, and 49, Zizzi as modified, still does not teach wherein the key

identifier associated with the column is stored as metadata associated with a table containing the

column within the database system.

Sutter teaches wherein the key identifier associated with the column is stored as metadata

associated with a table containing the column within the database system (see column 59, line 29

through 60, line 25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Zizzi as modified, to include wherein the key

identifier associated with the column is stored as metadata associated with a table containing the

column within the database system.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Zizzi as modified, by the teachings of Sutter because

wherein the key identifier associated with the column is stored as metadata associated with a

table containing the column within the database system would allow the same key to be used

with the same key algorithm to encrypt multiple columns of the same table or multiple columns

in different tables (see Sutter, column 60, lines 20-24).

As to claims 32, 41, and 50 Zizzi as modified, teaches further comprising establishing

encryption parameters for the column (see Sutter, column 60, lines 1-10), wherein encryption

parameters include encryption mode, key length, and integrity type (see <u>Sutter</u>, column 59, line

10-15, where different types of encryption are used to verify the integrity of the file) by:

entering encryption parameters for the column manually (see <u>Zizzi</u>, column 7, line 64

through column 8, line 6); and

recovering encryption parameters for the column from a profile table in the database

system (see <u>Zizzi</u>, column 8, lines 59-67).

As to claims 33, 42, and 51, <u>Zizzi</u> as modified, teaches wherein upon receiving a request

from the security administrator specifying the column to be encrypted (see <u>Sutter</u>, column 60,

lines 1-26, where "administrator" is read on "designer"), if the column currently contains data,

the method further comprises:

decrypting the column using an old key if the column was previously encrypted (it is

obvious to one skilled in the art that the column would have to be decrypted before the old key

could be discarded); and

encrypting the column using a new key (see <u>Sutter</u>, column 60, lines 1-19).

6.   Claims 29, 38, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over

<u>Zizzi</u> (U.S. patent No. 6,185,681 B1) in view of <u>McBride</u> (U.S. patent No. 6,292,899 B1) in

further view of <u>Sutter</u> (U.S. patent No. 5,924,094) as applied to claims 26-28, 30-33, 35-37, 39-

42, 44-46, and 48-51 above, and further in view of <u>Brogliatti et al.</u> (U.S. patent No. 6,564,225

B1).

As for claims 29, 38, and 47, <u>Zizzi</u> as modified, still does not teach wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

<u>Brogliatti et al.</u> teaches wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles (see column 5, lines 10-24).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified <u>Zizzi</u> as modified, to include wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified <u>Zizzi</u> as modified, by the teachings of <u>Brogliatti et al.</u> because wherein the security administrator, a database administrator, and a user administrator are distinct roles, and wherein a person selected for one of these roles is not allowed to be selected for another of these roles would protect important corporate assets (see <u>Brogliatti et al.</u>, column 5, lines 10-14).

Response to Arguments

7.   Applicant's arguments filed on 22 March 2004 with respect to rejected claims in view of the cited references have been fully considered but they are moot in view of the new ground of rejection.

Conclusion

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The

examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
6 May 2004

**SAM RIMELL
PRIMARY EXAMINER**